PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 6 : G07F 7/10

A1

(11) Numéro de publication internationale: **WO 97/42610**

(43) Date de publication internationale: 13 novembre 1997 (13.11.97)

(21) Numéro de la demande internationale: PCT/FR97/00826

(22) Date de dépôt international: 7 mai 1997 (07.05.97)

(30) Données relatives à la priorité:
96/05706 7 mai 1996 (07.05.96) FR

(71) Déposants *(pour tous les Etats désignés sauf US)*: FRANCE TELECOM [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR). LA POSTE [FR/FR]; 4, quai du Point du Jour, F-92777 Boulogne Billancourt (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(US seulement)*: PAILLES, Jean-Claude [FR/FR]; 4, rue des Loisirs, F-14610 Epron (FR). GIRAULT, Marc [FR/FR]; 9, rue Bernard Vanier, F-14000 Caen (FR). REMERY, Patrick [FR/FR]; 43, rue de Cornouailles, F-14000 Caen (FR).

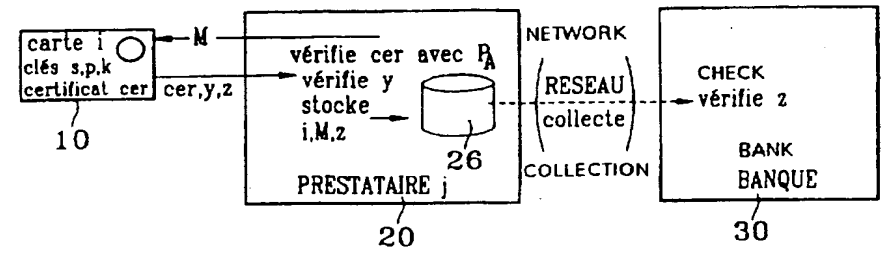
(74) Mandataire: SOCIETE DE PROTECTION DES INVENTIONS; 25, rue de Ponthieu, F-75008 Paris (FR).

(81) Etats désignés: JP, US, brevet européen (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée
Avec rapport de recherche internationale.
Avant l'expiration du délai prévu pour la modification des revendications, sera republiée si de telles modifications sont reçues.

(54) Title: METHOD FOR PERFORMING A DOUBLE-SIGNATURE SECURE ELECTRONIC TRANSACTION

(54) Titre: PROCEDE DE REALISATION D'UNE TRANSACTION ELECTRONIQUE SECURISEE A DOUBLE SIGNATURE



10... CARD I
KEYS s,p,k
CERTIFICATE cer
20... CHECK cer WITH P_A
CHECK y
STORE I,M,z
PAYEE j

(57) Abstract

A double-signature electronic transaction method is disclosed. Data is signed by the card (10) using a public key algorithm comprising proof (z) that the card has been debited, said proof (z) being a function f(k, M) of a parameter (M) and a secret debit key (k). A terminal (20) thus stores but cannot check the proofs (z) of various transactions. A central system (30) collects the proofs (z), checks them using the secret debit key (k), and credits the payee (20) only when the result of the check is positive. The method is particulary useful for producing électronic purses.

BNSDOCID: <WO 9742610A1 I >

(57) Abrégé

Procédé de réalisation d'une transaction électronique. Le procédé est à double signature. Les données signées par la carte (10) à l'aide d'un algorithme à clé publique comportant une preuve (z) que le débit de la carte a été effectué, cette preuve (z) étant une fonction f(k)M d'un paramètre M et d'une clé secrète de débit (k). Le terminal (20) stocke ainsi les diverses preuves (z) des diverses transactions effectuées mais ne peut vérifier ces preuves (z). Le système centralisé (30) collecte ces preuves (z) et les vérifie à l'aide de la clé secrète de débit (k), et ne crédite le prestataire (20) qu'en cas de vérification positive. Application notamment à la réalisation de porte-monnaie électronique.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce	ML	Mali	TR	Turquie
BG	Bulgarie	HU	Hongrie	MN	Mongolie	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MR	Mauritanie	UA	Ukraine
BR	Brésil	IL	Israël	MW	Malawi	UG	Ouganda
BY	Bélarus	IS	Islande	MX	Mexique	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	NE	Niger	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NL	Pays-Bas	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norvège	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NZ	Nouvelle-Zélande	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	PL	Pologne		
CM	Cameroun	KR	République de Corée	PT	Portugal		
CN	Chine	KZ	Kazakstan	RO	Roumanie		
CU	Cuba	LC	Sainte-Lucie	RU	Fédération de Russie		
CZ	République tchèque	LI	Liechtenstein	SD	Soudan		
DE	Allemagne	LK	Sri Lanka	SE	Suède		
DK	Danemark	LR	Libéria	SG	Singapour		
EE	Estonie						

PROCEDE DE REALISATION D'UNE TRANSACTION ELECTRONIQUE SECURISEE A DOUBLE SIGNATURE

DESCRIPTION

Domaine technique

La présente invention a pour objet un procédé de réalisation d'une transaction électronique sécurisée à double signature.

L'invention trouve une application dans tous les cas où des terminaux ont à traiter, de façon sécurisée, des transactions avec des utilisateurs munis de cartes à puce, ces terminaux n'étant pas en connexion permanente avec des systèmes de traitement centralisés, mais seulement périodiquement, lors de la collecte des transactions effectuées depuis la dernière collecte.

Etat de la technique antérieure

Pour faciliter l'exposé, l'exemple sera pris des transactions liées au paiement électronique et notamment à ce qu'il est convenu d'appeler le "porte-monnaie électronique", ou PME en abrégé. Pour ces techniques, on pourra se reporter à la revue "L'Echo des Recherches", numéro spécial 158, 4ème trimestre 1994, consacré au paiement électronique. Dans ce numéro, on pourra se reporter plus spécialement à l'article intitulé "Signature électronique et application au paiement électronique" par Marc GIRAULT et Luc VALLEE.

La technique du PME se développe depuis quelques années, mais la sécurité de ce genre d'applications pose encore des problèmes et suscite donc encore des

recherches. Différentes solutions sont possibles, qui peuvent être analysées sous l'angle du rapport sécurité/coût.

On peut rappeler que, dans ce type de systèmes, une carte porte-monnaie contient un solde (ou balance), c'est-à-dire certaine quantité de valeurs (monnaie, jetons, unités de consommation) et que, lors d'un paiement d'un montant m, ce solde est diminué de m unités ; la carte produit une preuve du débit de m unités, qui constitue une garantie de paiement du commerçant possédant le terminal (ou serveur), sur lequel l'utilisateur effectue la transaction. Cette preuve va conditionner le paiement du commerçant en monnaie normale, par l'autorité ayant émis les porte-monnaie électroniques, autorité que l'on peut appeler "la banque".

Cette preuve doit être vérifiée de façon à éviter des fausses cartes : il ne doit pas être possible de créer de toute pièce (c'est-à-dire sans carte) une preuve susceptible d'être reconnue comme étant authentique. Cette preuve doit aussi éviter des manipulations, telles que la transformation d'un montant m en un montant m' supérieur à m, ou la réutilisation de la même preuve pour payer par exemple deux fois le montant dû au commerçant, ou payer de façon indue d'autres commerçants.

Dans la suite de la description, on désignera les différents acteurs de ces systèmes respectivement par "utilisateur", "prestataire" et "banque". L'utilisateur possède donc une carte PME pour payer un prestataire. La banque est l'entité qui émet les PME.

BNSDOCID: <WO 9742610A1 | >

Les techniques utilisées aujourd'hui peuvent être classés schématiquement en trois catégories, selon qu'elles utilisent des signatures à clé secrète, à clé publique ou à clés interactives.

Pour ce qui est des premières, on peut distinguer le cas où le terminal est déconnecté de la banque (autrement dit est autonome, ou en terminologie anglo-saxonne, "offline") du cas où le terminal est connecté directement à la banque. Le premier cas (déconnecté ou "offline") est le plus courant dans les différents systèmes de porte-monnaie existants. Il consiste à calculer la preuve z avec un algorithme à clé secrète f, sur le paramètre i représentant le numéro de la carte PME, et sur un paramètre M, qui désigne l'ensemble des paramètres suivants :

m : le montant de la transaction ;

j : le numéro du module de sécurité (appelé généralement "Secure Application Module" ou SAM en abrégé) ;

r : un aléa ou plus simplement le contenu d'un compteur.

On a donc $z=f(k,m,j,r)$ où k est la clé secrète du PME d'identité i, clé qui dépend de i par un mécanisme de diversification des clés selon le numéro i de carte. Le module SAM est une carte à puce située dans le terminal, qui joue le rôle de caisse enregistreuse sûre et protégée grâce aux qualités de sécurité physique des cartes à puce utilisées. Ce module SAM contrôle donc le certificat z et accumule les montants. Il est régulièrement vidé pour que le prestataire fasse enregistrer ses gains auprès de la banque, grâce à une procédure sécurisée entre le module SAM et la banque,

qui n'offre pas de difficultés particulières et qui ne sera donc pas décrite ici.

Pour contrôler le certificat z, le module SAM doit connaître les clés de toutes les cartes PME , ce qui, en pratique, est obtenu en calculant les clés k des PME par une formule de diversification k=g(KM,i), où KM est une clé maître, valable pour tout le système, et qui est dans tous les modules SAM.

Ce mode de mise en oeuvre est illustré sur la figure 1 annexée où la carte PME de l'utilisateur porte la référence 10, le terminal du prestataire la référence 20, avec son module SAM 25, et la banque la référence 30. La flèche dirigée du terminal 20 vers la carte 10 représente la transmission des paramètres M vers la carte et la flèche dirigée en sens contraire représente la transmission du certificat z vers le terminal.

Ce premier mode de mise en oeuvre présente l'avantage de conduire à des cartes de coût faible. Mais il présente quelques inconvénients :

- la sécurité est liée à l'impossibilité de lire dans le module SAM la clé maître KM, donc sur la sécurité physique des modules SAM, lesquels sont très répandus puisque situés dans tous les terminaux. Or, cette sécurité est difficile à garantir. La connaissance de la clé maître KM permettrait de réaliser des fraudes de grande ampleur, en fabiquant des cartes de numéro i quelconque, qu'aucun mécanisme de liste noire ne permettrait de stopper ;
- les modules SAM sont situés dans les terminaux, ou chez les serveurs, ce qui pose des problèmes

BNSDOCID: <WO 9742610A1_I_>

pratiques lorsqu'il faut accepter plusieurs types de cartes PME, avec chacune leur SAM ; c'est le cas très répandu dans la pratique, où il n'y a pas qu'une seule banque mais plusieurs, susceptibles d'émettre leurs propres cartes PME.

Pour ce qui est maintenant du cas où le terminal du prestataire est connecté à la banque ("online"), le module de sécurité SAM n'existe plus dans le terminal, et le contrôle du certificat doit se faire dans la banque. Cette solution est illustrée sur la figure 2 annexée avec les mêmes références que sur la figure 1.

Cette solution n'est pas très intéressante en pratique, car elle entraîne des coûts de télécommunication importants. Or, un porte-monnaie électronique doit rester un moyen de paiement rentable, même pour des transactions portant sur de très petits montants.

Pour ce qui est maintenant des systèmes utilisant un procédé de signature avec algorithme à clé publique, on peut encore distinguer deux cas selon que l'on utilise ou non un module de sécurité SAM.

Si l'on n'utilise pas de module SAM, le certificat z des systèmes précédents utilisant des clés sécrètes est remplacé par une signature basée sur un algorithme à clé publique tel que l'algorithme RSA ("Rivest-Shamir-Adleman"). Chaque carte possède un couple de clés sécrète et publique, respectivement s et p, et la preuve du débit défini par le paramètre M est obtenue par le calcul d'une signature y=s(M).

Cette signature peut être vérifiée par le prestataire, en utilisant la clé publique. Toutes les

signatures peuvent être stockées, puis collectées périodiquement pour faire enregistrer les paiements par la banque. Dans ce type de réalisation, il faut aussi que la clé publique p soit certifiée par l'autorité qui émet les cartes, car le fait de posséder un couple de clés s et p ne prouve pas qu'il s'agisse d'une carte PME authentique : il est en effet facile de trouver de tels couples avec, par exemple, des logiciels sur calculateur personnels adaptés. Il faut donc que le PME transmette au terminal non seulement sa clé publique p, mais aussi un certificat lié à la clé publique p. Dans la suite, on notera "cer" ce certificat. Le certificat "cer" est vérifié avec la clé publique PA de la banque.

La figure 3 annexée illustre cette variante. Les références sont les mêmes, mais on note, dans le terminal 20 du prestataire, un moyen de collecte (ou de mémorisation) 26 capable de stocker les numéros des cartes i, les paramètres M, les certificats cer et les signatures y.

L'avantage de ce système tient à ce qu'il n'existe plus de clé maître secrète dans les terminaux, avec les risques que cela comportait, ni de modules SAM. Le système est donc plus sûr et présente une meilleure flexibilité.

Mais ce système présente des inconvénients :

- le coût des cartes capables de faire des calculs fondés sur des algorithmes à clé publique de type RSA est élevé, car la puissance de calcul nécessaire, à temps de réponse donné, est importante ;
- la quantité de données à mémoriser dans le terminal et à collecter est importante : en

PNSDOCID: <WO 9742610A1 | >

effet, par transaction, il faut mémoriser M, et y ; cet ensemble de données représente, avec les longueurs courantes de clés publiques (512 bits, un ensemble de l'ordre de 1,5 kbits.

Dans la variante avec module de sécurité SAM, on accumule les transactions dans le terminal et on les fait collecter ensuite par la banque. L'opération d'accumulation étant sensible du point de vue sécurité, puisqu'une fraude tentante serait de modifier chez le prestataire le montant accumulé, il est nécessaire d'avoir un module SAM qui vérifie les signatures des transactions et les accumule.

La figure 4 annexée illustre cette variante avec les mêmes références.

L'avantage de cette variante tient à ce qu'il n'y a plus de clé maître secrète dans le terminal, ce qui conduit à une meilleure sécurité. Mais des inconvénients demeurent, qui sont doubles :

- le coût des cartes capables de faire des calculs fondés sur des algorithmes à clé publique est élevé, car la puissance de calcul nécessaire, à temps de réponse donné, est importante,
- il est nécessaire d'utiliser un module SAM.

La troisième catégorie de procédés concerne les procédés utilisant des schémas de signature interactive. L'utilisation de cette technique permet de réduire considérablement la puissance de calcul nécessaire dans les cartes : le rapport est de 10 à 20 avec les paramétrages couramment utilisés. A puissance de calcul identique, les temps de réponse sont donc

meilleurs. A temps de réponse identique, le coût des composants des cartes PME est moins élevé.

On utilise en général deux types de schémas d'authentification, l'un dit de GUILLOU-QUISQUATER (ou GQ en abrégé), l'autre dit de FIAT-SHAMIR (ou FS en abrégé). Le numéro de l'Echo des Recherches cité plus haut contient toutes les références bibliographiques à ce sujet.

On rappelle brièvement en quoi consiste un schéma de signature de ce type en prenant un exemple emprunté au schéma GQ. Dans ce schéma, la carte, notée Ci, utilise les fonctions ou paramètres suivants :

g : fonction d'expansion de 64 en 512 bits,

h : fonction de hâchage ("hashing") : résultat sur 64 bits,

* : opération de restriction à 128 bits poids faible,

S_A et P_A : clés secrète et publique de l'autorité : 768 bits,

i : identité de la carte, sur 64 bits,

n : module sur 512 bits,

cer : $S_A(i,n,e)$ sur 768 bits,

e : n nombre premier à 16 bits,

v : $1/I^{1/e}$ mod n, sur 512 bits.

Le terminal sécurisé Tj possède la clé publique P_A, g, h et est identifié par j, sur 64 bits.

Les opérations mises en oeuvre sont alors les suivantes :

1) le terminal fixe le montant m de la transaction, tire un aléa r et constitue le paramètre M rassemblant m, j et r, et transmet M à la carte ;

BNSDOCID: <WO 9742610A1 | >

2) la carte vérifie que son solde (ou balance) est supérieur au montant m de la transaction ; si c'est le cas, la carte tire un aléa x, calcule $t=x^e \bmod n$ et $b=h(t^*,M)$ et transmet au terminal i, b et le certificat $cer=S_A(i,n,e)$;

3) le terminal vérifie le certificat et obtient i, n et e, choisit un nombre c aléatoire inférieur à e et envoie c à la carte ;

4) la carte calcule $y=xv^c \bmod n$ et réduit son solde de m et transmet au terminal y et t^* ;

5) le terminal calcule $I=g(i)$, calcule la quantité $u=(y^e I^c \bmod n)^*$ puis $h(u,M)$ et vérifie que b est égal à $h(u,M)$; alors le terminal augmente son solde de m.

On peut résumer ce schéma à l'essentiel de la manière suivante :

- la carte choisit un aléa x, calcule $t=x^e$ modulo n et envoie au terminal $b=h(M,t)$,
- le terminal choisit alors un aléa c tel que $0<c<e$ et l'envoie à la carte,
- la carte répond alors par $y=xv^c$ modulo n,
- le terminal vérifie alors que si $u=y^e I^c$, alors $b=h(M,u)$ (car $v^e I=1 \bmod n$).

Ce schéma est illustré sur la figure 5 annexée. Son intérêt réside dans le fait que la puissance de calcul requise est inférieure au cas des schémas de type RSA. Mais un inconvénient subsiste, car ce schéma nécessite un module SAM. En effet, la signature interactive n'a de valeur que si l'on est sûr que l'aléa c a bien été soumis à la carte et dans l'ordre indiqué. Les signatures interactives sont dites, pour cette raison, jetables : elles ne sont utilisables

qu'au moment où elles sont obtenues. En effet, la signature interactive comprend les données M, cer, b, c, y. Or, il est facile de créer ces données de toute pièce : connaissant cer et M, on a p et r, et il suffit de choisir y et c et de calculer $t=y^{e}r^{c}$ et b=h(M,t) ; les données obtenues M, cer, b, c, y constituent une signature valide.

Le but de la présente invention est justement de remédier à ces inconvénients.

Exposé de l'invention

A cette fin, l'invention propose un procédé à double signature, l'une du type à clé publique ou secrète (notée y dans les schémas précédents), l'autre basée sur un algorithme à clé secrète (notée z dans les schémas précédents). Cette double signature est conçue de façon à combiner les avantages des deux techniques et implique donc une combinaison judicieuse de ces signatures et des éléments signés, de façon à conduire effectivement aux avantages recherchés.

Comme il a été expliqué plus haut, dans un schéma de signature de type RSA, la preuve du débit de la carte est obtenue par le calcul de la signature y=s(M) et cette signature peut être vérifiée par le prestataire, sans que celui-ci ait à contenir de secrets (il travaille avec la clé publique). C'est ce qui est illustré sur la figure 3.

Dans un schéma de signature à clé secrète, la preuve z est obtenue par un algorithme à clé secrète en calculant z=f(k,m,j,r) où k est la clé secrète et, dans la variante sans SAM, z n'est pas vérifiable par le prestataire mais seulement par la banque. Cette preuve

BNSDOCID: <WO 9742610A1 I.>

z, avec i et M, doit être stockée par le prestataire puis collectée par la banque.

Selon l'invention, on combine ces deux schémas de telle sorte que la signature y, que le prestataire peut vérifier, dépende de la signature z, non vérifiable par le prestataire. On a ainsi $y=s(M,z)$ au lieu de $y=s(M)$. Ainsi, une modification de z en z' par l'utilisateur nécessiterait de modifier y en $y'=s(M,z')$ ce qui est impossible puisque la fonction s n'est connue que de la carte.

Dans un schéma de signature interactive, au lieu de calculer dans la carte la fonction $b=h(M,t)$ comme expliqué plus haut, avec $t=x^e \bmod n$, on calculera une fonction b qui inclut la preuve z, soit $b=h(M,t,z)$. Si z est modifié par l'utilisateur en z', alors le logiciel du prestataire s'en apercevra. En effet, t n'est dévoilé (indirectement) qu'à la fin de l'échange. L'utilisateur ne peut donc calculer $b'=h(M,t,z')$ au moment où b' devrait être envoyé au prestataire.

De manière précise, l'invention a donc pour objet un procédé de réalisation d'une transaction électronique entre un utilisateur possédant une carte, un prestataire possédant un terminal apte à recevoir cette carte et un système centralisé apte à être connecté périodiquement au terminal, procédé dans lequel :

- le terminal transmet à la carte un paramètre comprenant au moins le montant de la transaction,
- la carte débite son solde dudit montant,
- la carte et le terminal calculent et échangent diverses données dont certaines sont signées par

la carte au moyen d'un algorithme à clé publique ou secrète,

- le terminal vérifie les données signées par ledit algorithme à clé publique ou secrète et stocke les paramètres propres aux diverses transactions réalisées,
- le système centralisé collecte périodiquement les données stockées lorsqu'il est connecté au terminal et crédite le prestataire des montants correspondants,

ce procédé étant caractérisé par le fait qu'il est à double signature, les données signées par la carte à l'aide de l'algorithme à clé publique ou secrète comportant une preuve z que le débit de la carte a été effectué, cette preuve z étant une fonction du paramètre et d'une clé secrète de débit, le terminal stockant ainsi, en outre, les diverses preuves des diverses transactions effectuées mais ne pouvant vérifier ces preuves, le système centralisé collectant, en outre, ces preuves et les vérifiant à l'aide de la clé secrète de débit, et ne créditant le prestataire qu'en cas de vérification positive.

Si le paiement est fait en ligne avec un serveur prestataire, l'algorithme peut être à clé secrète.

Brève description des dessins

- la figure 1, déjà décrite, illustre un schéma connu de signature avec algorithme à clé secrète avec terminal déconnecté ;
- la figure 2, déjà décrite, illustre un schéma connu de signature avec algorithme à clé secrète avec un terminal connecté à la banque ;

BNSDOCID: <WO___9742610A1_I_>

- la figure 3, déjà décrite, illustre un schéma connu de signature avec algorithme à clé publique sans module de sécurité ;
- la figure 4, déjà décrite, illustre un schéma connu de signature avec algoritime à clé publique avec module de sécurité ;
- la figure 5, déjà décrite, illustre un schéma connu de signature interactive ;
- la figure 6 illustre un premier mode de mise en oeuvre de l'invention dans le cas d'un schéma de signature de type à clé publique ;
- la figure 7 illustre un second mode de mise en oeuvre de l'invention dans le cas d'un schéma de signature interactive.

Exposé détaillé d'un mode de mise en oeuvre

On va décrire, à titre d'exemple, un mode de mise en oeuvre fondé sur une signature interactive. Les notations seront les suivantes :

g : fonction d'expansion 48 en 512 bits ;

h : fonction de hâchage : résultat 128 bits ;

f : fonction de calcul de signature à clé secrète (comme DES par exemple) : 64 bits ;

τ : restriction à k.64 bits de poids faible ; k paramètrable de 4 à 8 ;

S_A et P_A : clés secrète et publique de l'autorité : 768 bits.

Les données contenues dans la carte sont les suivantes :

i : identité de la carte : 48 bits

n : module : 512 bits

cer : $S_A(i,n,e)$: certificat de 768 bits

e : $2^{16}+1$

v : $1/I^{1/e}$ mod n : 512 bits

k : clé secrète de débit, 64 bits

bal : solde de la carte : 32 bits

h, f.

Les données contenues dans le terminal du prestataire sont les suivantes :

P_A, g, h

j : identité du terminal : 48 bits

m : montant : 16 bits

r : contenu du compteur : 32 bits

Les opérations successives sont alors les suivantes :

1) Le terminal du prestataire fixe le montant m de la transaction et constitue M à l'aide de m, j et le contenu r du compteur, et fait passer à r+1 ce contenu ; le prestataire transmet M à la carte.

2) La carte vérifie que le solde n'est pas inférieur au montant m. Si c'est bien le cas, la carte choisit un aléa x de 512 bits, calcule $t=x^e$ mod n, calcule la preuve z à l'aide de la clé secrète de débit k, soit $z=f(k,M)$, calcule également $b=h(t^*,M,z)$, débite le solde du montant m, enregistre M ; la carte possède le certificat de l'autorité $cer=S_A(i,n,e)$ où S_A est la clé secrète de l'autorité ; la carte transmet finalement au terminal du prestataire la preuve z, la fonction f et le certificat cer.

3) Le terminal du prestataire vérifie le certificat cer à l'aide de la clé publique de l'autorité P_A et obtient n, e, et I ; il choisit un nombre c

RNSDOCID: <WO 9742610A1_I_>

aléatoire appelé aussi chalenge, sur 16 bits et transmet c à la carte.

4) La carte calcule $y=xv^c \bmod n$ et transmet y au terminal du prestataire.

5) Le terminal du prestataire calcule I=g(i), puis $u=(y^e I^c \bmod n)^*$; il vérifie que b est égal à h(u,M,z) et, si c'est le cas valide la transaction. Ce terminal collecte i, M et z et envoie ces données à la banque.

6) La banque, avec i, retrouve la clé secrète de débit k et vérifie la preuve z=f(k,M). La banque vérifie que le compteur r du terminal du prestataire j progresse et si c'est le cas crédite le compte du prestataire j du montant m.

Ce schéma peut être modifié en rendant la signature interactive non jetable et cela en changeant $z=f(k,M)$ en $z=f(k,M,t^*)$. La méthode de création d'une signature interactive (i,M,cer,y,z) décrite plus haut ne fonctionne alors plus : on choisit y, c et M ; on calcule $t^*=(y^e I^c \bmod n)^*$; on calcule b=h(t*,M,z) mais t ne satisfera pas à $z=f(k,M,t^*)$. Les données i, M, z, t*, b, c, y ont alors à être mémorisées chez le prestataire.

Le niveau de sécurité du protocole précédent est lié à la taille du challenge c : par exemple, si c fait 16 bits, il y a une chance sur $2^{16}=65536$ pour qu'un émulateur de cartes, en devinant c, puisse créer artificiellement une transaction. Le temps de calcul de la carte est aussi directement proportionnel à ce niveau de sécurité. Le niveau de sécurité peut être adapté en faisant varier la longueur du nombre

aléatoire c transmis par le terminal à la carte dans le cas de la signature interactive. Un perfectionnement consiste donc à faire en sorte que le prestataire ajuste le niveau de sécurité en fonction de paramètres tels que le montant de la transaction, la possibilité d'avoir des utilisateurs avec des fausses cartes, bien plus importante pour du télépaiement que du paiement de contact, etc...

On voit après cette description que le procédé de l'invention présente de nombreux avantages :

- il est peu consommateur de puissance de calcul : donc, à performances égales, les cartes PME seront moins chères, ou, à puissance égale, la vitesse sera plus grande,
- il est utilisable sans module SAM chez les prestataires,
- il minimise la quantité de mémoire de stockage chez le prestataire (rapport 5 à 10),
- il réduit dans les mêmes proportions la quantité d'informations à transporter du prestataire à la banque,
- il est utilisable avec un module SAM, s'il est jugé préférable d'accumuler les transactions chez le prestataire, mais ce module SAM ne contenant pas de clés secrètes, est peu sensible,
- il est ajustable en niveau de la sécurité, suivant les caractéristiques des transactions.

On pourrait penser qu'un niveau de sécurité de 2^{16} est faible comparé aux niveaux habituels de la cryptographie, où il est courant de prendre des aléas sur 64 voire 512 bits. Il faut cependant noter que, concernant le coût de recherche de la clé (ici v),

RNSDOCID: <WO 9742610A1_I_>

c'est-à-dire le nombre d'itérations à réaliser pour trouver la clé, à partir d'un couple challenge-réponse, le système proposé a exactement les mêmes caractéristiques de sécurité que les systèmes classiques. Pour mettre à profit ce niveau de sécurité de 2^{16}, il faudrait, avec une fausse carte, attendre en moyenne 32 000 transactions rejetées avant d'en avoir une acceptée.

REVENDICATIONS

1. Procédé de réalisation d'une transaction électronique entre un utilisateur possédant une carte (10), un prestataire possédant un terminal (20) apte à recevoir cette carte (10) et un système centralisé (30) apte à être connecté périodiquement au terminal (20), procédé dans lequel :

- le terminal (20) transmet à la carte un paramètre (M) comprenant au moins le montant (m) de la transaction,
- la carte (10) débite son solde du montant (m),
- la carte (10) et le terminal (20) calculent et échangent diverses données dont certaines sont signées par la carte au moyen d'un algorithme à clé publique ou secrète,
- le terminal (20) vérifie les données signées par ledit algorithme à clé publique ou secrète et stocke les paramètres propres aux diverses transactions réalisées,
- le système centralisé (30) collecte périodiquement les données stockées lorsqu'il est connecté au terminal et crédite le prestataire des montants correspondants,

ce procédé étant caractérisé par le fait qu'il est à double signature, les donnés signées par la carte (10) à l'aide de l'algorithme à clé publique ou secrète comportant une preuve z que le débit de la carte a été effectué, cette preuve z étant une fonction f(k,M) du paramètre M et d'une clé secrète de débit (k), le terminal (20) stockant ainsi, en outre, les diverses preuves z des diverses transactions effectuées mais ne pouvant vérifier ces preuves (z), le système centralisé

(30) collectant, en outre, ces preuves (z) et les vérifiant à l'aide de la clé secrète de débit (k), et ne créditant le prestataire (20) qu'en cas de vérification positive.

2. Procédé selon la revendication 1, caractérisé par le fait que l'une des signatures qu'il utilise est une signature de type RSA et par le fait que la carte (10) possède un certificat de l'autorité (cer) des paramètres (n,e) de la clé publique (p) et de l'identité (i) de la carte, et calcule la signature $y=s(M,z)$ et transmet au terminal (20) le certificat (cer), la signature y et la preuve z, le prestataire vérifiant cer et y, stockant i,M et z et le système centralisé vérifiant les preuves (z).

3. Procédé selon la revendication 1, caractérisé par le fait que l'une des signatures qu'il utilise est une signature interactive et qu'il comprend les opérations suivantes :

- la carte (10) possède un certificat de l'autorité (cer) des paramètres (n,e) de la clé publique et de l'identité (i) de la carte, choisit un aléa (x), calcule $t=x^e \bmod n$ où e et n définissent la clé publique (p), calcule la preuve $z=f(k,M)$ à l'aide de la clé secrète de débit k, calcule $b=h(t^*,M,z)$ où t^* est une restriction de t à des bits de poids faible, et transmet au terminal (20) la preuve (z), le nombre b, et le certificat (cer),
- le terminal (20) vérifie le certificat (cer) à l'aide de la clé publique (p_A) et obtient n, e,

i, tire un nombre aléatoire c ayant une certaine longueur et transmet c à la carte (10),

- la carte (10) calcule $y=x.v^c \bmod n$ et transmet y au terminal (20),
- le terminal calcule $I=g(i)$ où g est une fonction d'expansion, calcule $u=(y^e I^c \bmod n)^*$ et vérifie que $b=h(u,M,z)$, et stocke i, M et z,
- le système centralisé vérifie les preuves (z).

4. Procédé selon la revendication 3, caractérisé par le fait que le niveau de sécurité de la première signature est adapté en faisant varier la longueur du nombre aléatoire c.

FIG.1

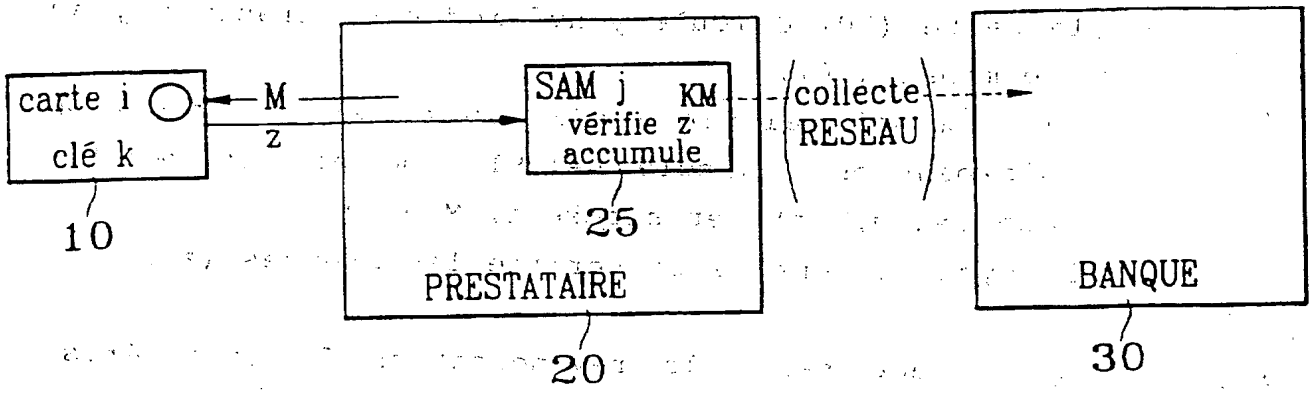


FIG.2

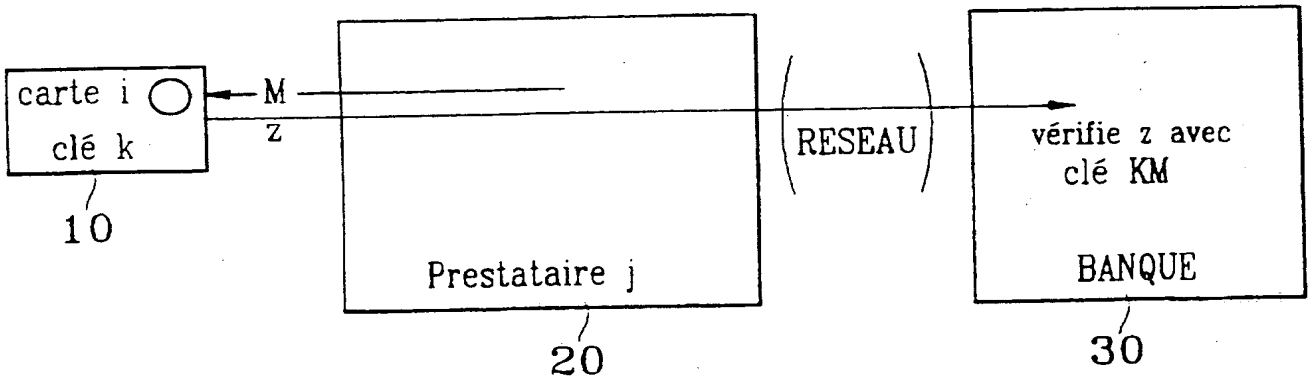


FIG.3

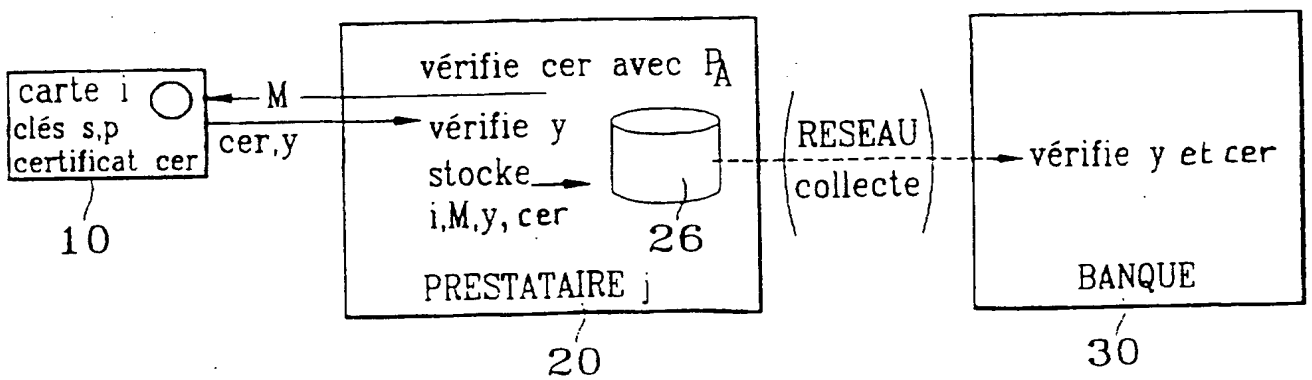


FIG. 4

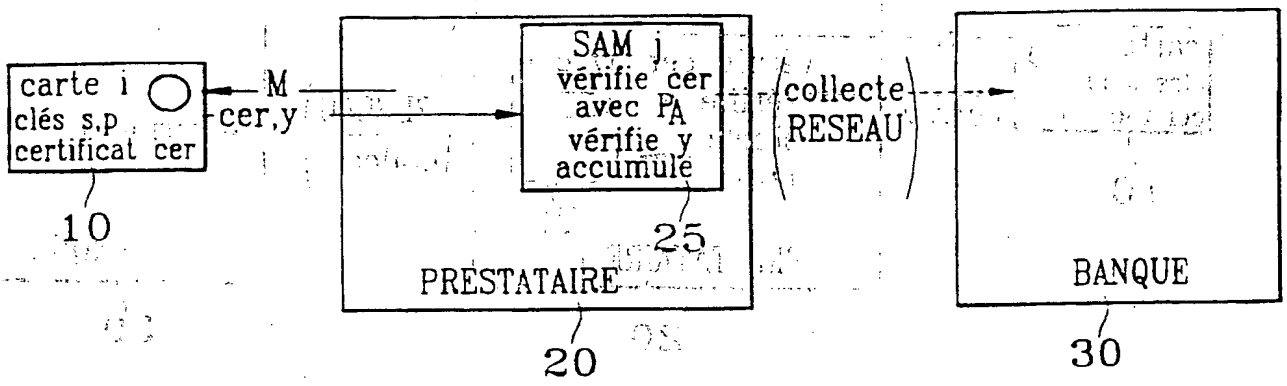
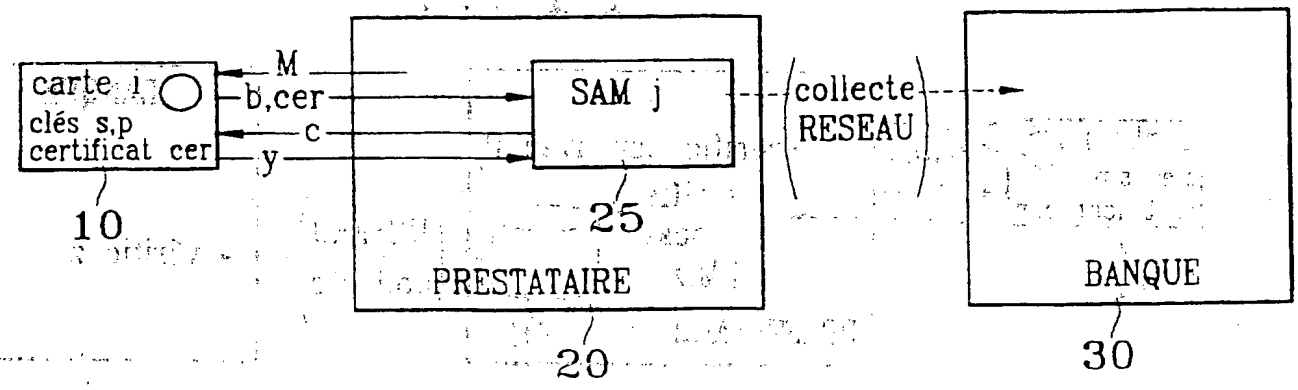


FIG. 5



BNSDOCID: <WO___9742610A1_I_>

FIG.6

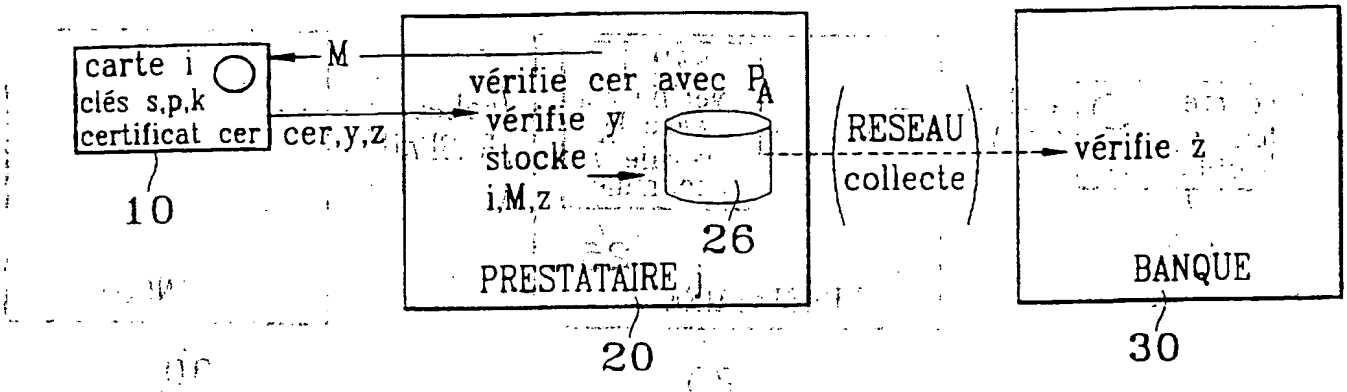
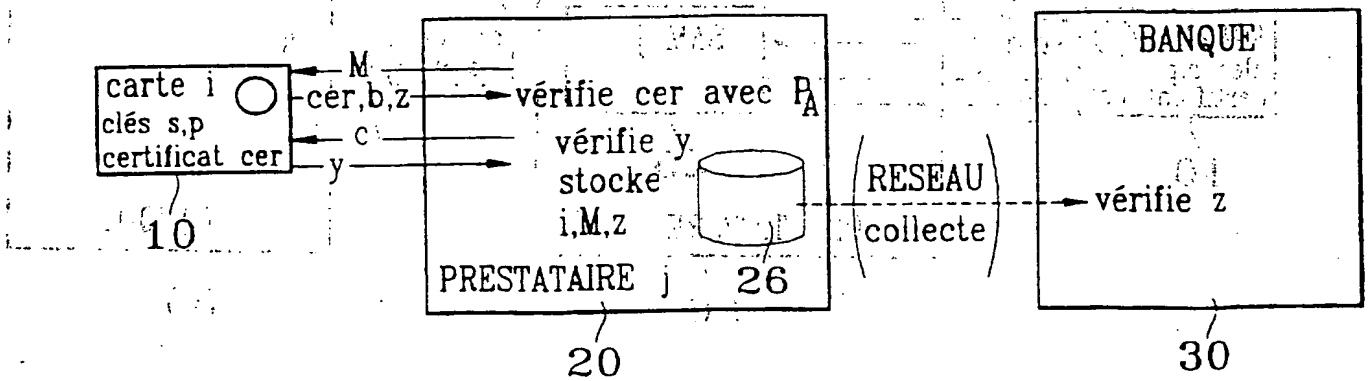

carte i
clés s,p,k
certificat cer
M
cer,y,z
vérifie cer avec P_A
vérifie y
stocke
i,M,z
26
PRESTATAIRE j
20
RESEAU
collecte
vérifie z
BANQUE
30
10

FIG.7


carte i
clés s,p
certificat cer
M
cer,b,z
c
y
vérifie cer avec P_A
vérifie y
stocke
i,M,z
26
PRESTATAIRE j
20
RESEAU
collecte
BANQUE
vérifie z
30
10

INTERNATIONAL SEARCH REPORT

Inter ial Application No
PCT/FR 97/00826

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 363 122 A (FUJITSU) 11 April 1990 see abstract; claims; figures 1-5 see column 7, line 26 - column 9, line 8	1,4
Y	GB 2 261 538 A (BANK OF SCOTLAND) 19 May 1993 see the whole document	1,4
A	EP 0 588 339 A (NIPPON TELEGRAPH AND TELEPHONE) 23 March 1994 see abstract; figures 5A-6,9 see column 9, line 57 - column 13, line 23 see column 15, line 43 - column 18, line 47	1-3
A	WO 93 08545 A (JONHIG) 29 April 1993 see abstract; claims; figures see page 11, line 8 - page 18, line 24	1,2

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 August 1997	12.09.97

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+ 31-70) 340-3016	David, J

Form PCT/ISA/210 (second sheet) (July 1992)

BNSDOCID: <WO ..._9742610A1_I_>

INTERNATIONAL SEARCH REPORT

Intern[illegible] Application No
PCT/FR 97/00826

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 496 656 A (FRANCE TELECOM) 29 July 1992	
A	EP 0 172 670 A (TECHNION RESEARCH & DEVELOPMENT) 26 February 1986	

Form PCT/ISA/210 (continuation of second sheet) (July 1992)*

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter[illegible]al Application No
PCT/FR 97/00826

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0363122 A	11-04-90	JP 2096872 A	09-04-90
		JP 6022030 B	23-03-94
		CA 1319432 A	22-06-93
		DE 68920107 D	02-02-95
		DE 68920107 T	11-05-95
		US 5097115 A	17-03-92
GB 2261538 A	19-05-93	NONE	
EP 0588339 A	23-03-94	JP 6103425 A	15-04-94
		JP 6103426 A	15-04-94
		JP 6162289 A	10-06-94
		JP 6162287 A	10-06-94
		JP 6161354 A	07-06-94
		US 5396558 A	07-03-95
		US 5446796 A	29-08-95
		US 5502765 A	26-03-96
WO 9308545 A	29-04-93	AT 145744 T	15-12-96
		AU 663739 B	19-10-95
		AU 2888692 A	21-05-93
		BR 9205416 A	17-05-94
		CA 2098481 A	17-04-93
		DE 69215501 D	09-01-97
		DE 69215501 T	27-03-97
		EP 0567610 A	03-11-93
		ES 2096772 T	16-03-97
		JP 6503913 T	28-04-94
		PL 299825 A	18-04-94
		US 5440634 A	08-08-95
EP 0496656 A	29-07-92	FR 2671889 A	24-07-92
		DE 69204696 D	19-10-95
		DE 69204696 T	02-05-96
		JP 6203226 A	22-07-94
		US 5247578 A	21-09-93
EP 0172670 A	26-02-86	JP 61094177 A	13-05-86

BNSDOCID: <WO 9742610A1 | >